UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,445	10/31/2001	Richard Paul Tarquini	10016861-1	2406

7590 09/22/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 09/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/001,445	TARQUINI ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to the amendment filed on June 27, 2005.

Claims 1-12 are pending.

2. The objection to the **drawing** has been withdrawn as the applicant made the appropriate correction.

3. The objection to claim 8 has been withdrawn as the applicant made the appropriate correction.

Response to Arguments

4. Applicant's argument filed on June 27, 2005 have been fully considered but they are not persuasive.

There are three independent claims in particular claims 1, 8 and 11. Claim 8 and 11 have been amended by the applicant and the following limitation has been added to the former independent claims 8 and 11, "the network filter service provider implemented as an intermediate driver of the network stack."

The first argument by the applicant is with regard to the independent claims 8 and 11. Applicant argued that the amended claim 8 and 11includes limitations that are not shown or suggested/anticipated by the references on the record, namely **Holland.**

Applicant wrote the following in support of his argument,

" Holland does not disclose or even suggest a network filter service provider implemented as an intermediate driver of the network stack" as recited by amended independent Claims 8 and 11 .

Holland appears to disclose a packet filter 37 that collects all network traffic

Transiting through the network interface controller (N1C) 31 of Holland (also referred to by the Examiner with respect to the rejection of Claims 1-7 under 35 U.S.C. 103 at page 8 of the Office Action) Holland, column 4, lines 52-53). Holland also appears to disclose that the NIC 31 of Holland is placed in standard mode such that NIC 31 ' all network traffic destined for the media access control (MAC) address (Holland, column 4, lines 53-55).

Holland further recites:

> The packet filter 37 captures and filters the data frames. A stream and packet processing module 38 demultiplexes the filtered data frames into individual frames, datagrams, and packets in accordance with the network protocols supported by the IP stack 33. In effect, the stream and packet processing module duplicates the functionality of the IP stack 33 by reassembling raw data frames into properly formatted, higher protocol data packets. These data packets are collected by a network collector 39 for use by the analysis module 36.

(Holland, column 4, lines 57-67, figure 2)(emphasis added). The Examiner also states that the protocol driver is inherently included in the IP stack" of Holland (Office Action, page 4). Thus, the filter 37 of Holland does not appear to be, or function as, an intermediate driver of a network stack where the network stack comprises a media access control driver and a protocol driver. To the contrary, the packet filter 37 of Holland does not appear to transfer any data to, or receive any data from, the IP stack 33 of Holland referred to by the Examiner (see, also, figure 2 of Holland). Thus, Applicants respectfully submit that Holland does not disclose or even suggest a network filter service provider implemented as an intermediate driver of the network stack" as recited by independent Claims 8 and 11."

Applicant also argued that that

the packet filter 37 of Holland is not an "intermediate driver" of a network stack comprising a protocol driver and a media access control driver.

Examiner disagrees with this argument, examiner would point out that added limitation made by amendment is still disclosed by the reference on the record namely Holland as shown below.

The network filter service provider [figure 2, ref. Num "37"] implemented as an intermediate driver of the network stack (The network filter service provider is implemented as an intermediate driver because it is bound to the protocol driver [figure 2, ref. Num "33"] and **the media access control driver**.[figure 2, ref. Num "31"] (With respect to **Holland** the Packet filter/an instance of the intrusion detection service which is shown on figure 2, ref. Num "37" is implemented as **an intermediate driver** and bound to the MAC driver which is inherently included in the NIC and to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num "33" and shown also on figure 3, ref. Num "52. This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num "82" and "83", namely the network layer and the transport layer are all implemented by the protocol driver.)

Examiner further points out the following facts as to how and why the filter service shown on figure 2, ref. Num "37" is actually considered as an intermediate driver.

- With respect to **Holland** the Packet filter service which is shown on figure 2, ref. Num "37" is binding to both the MAC driver which is inherently included in the NIC and the Packet filter is also binding to the protocol driver which is inherently

included in the IP stack shown on figure 2, ref. Num "33" and shown also on figure 3, ref. Num "52". This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num "82" and "83", namely the network layer and the transport layer are all implemented by the protocol driver.

In response to the argument made by the applicant that the packet filter does not appear to transfer any data to, or receive any data from, the IP stack 33.

Examiner would point out that the packet filter indeed transfer data or receive data as it captures and filters the data frames see what is disclosed on column 4, lines 52-58.

"A packet filter 37 collects all network traffic transiting through the NIC 31. The NIC 31 is left in standard mode, that is, a mode which copies out all network traffic destined for the media access control (MAC) address of that NIC 31 only and includes, but is not limited to, specified ports, inbound and outbound traffic, and specific protocols. **The packet filter 37 captures and filters the data frames"**

The rest of the argument by the applicant is with regard to the dependent claims. Applicant argued that the rest of the dependent claims are allowable for the reason that Holland does not disclose the limitation of claims 1, 8 and 11.

In response to the above argument by the applicant, the examiner response discussed for the independent claims 8 and 11 above is also valid towards this argument.

See the office action below for detailed explanation given for claim 1 and the rest of the claims.

Therefore all the elements of the limitations is explicitly/implicitly/inherently suggested and disclosed by primary reference "Holland" or by the combinations

of the references on the records namely, "Holland" and "Moran" and the rejection remains valid.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 8-12** are rejected under 35 U.S.C. 102(e) as being anticipated by **Holland III et al** (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061)

7. **As per claims 8 and 11, Holland discloses a method of performing intrusion prevention** [figure 1, ref. Num "20", ref. Num "19", ref. Num 18"] **at a node** [figure 1, ref. Num "11"' ref. Num "12"] **of a network** [figure 1, ref. Num 10], **comprising**:

- **Binding a network filter service provider** [figure 2, ref. Num "37"] **to a media access control driver of a network stack of the node** [figure 2, ref. Num "31"; column 4, lines 53-57] (The MAC driver is inherently included in the NIC. The MAC or the "media access control driver", also called the "network card driver", allows the operating system to talk with the NIC.

Windows NT and Windows 95/98 come with MAC drivers for most NICs. The MAC driver got its name from the fact that it operates at the lower level of the OSI model. The second layer of the model, the Data Link layer, is divided into two pieces: the LLC and MAC. The LLC sub layer is implemented in the transport driver while the MAC sub layer is implemented in the NIC); and

- **Binding the network filter service provider** [figure 2, ref. Num "37"] **to a protocol driver of a network stack of the node**. [Figure 2, ref. Num "33" or figure 3, ref. Num "52"; and figure 4, ref. Num "82" and ref. Num "83"; Column 6, lines 27-31](The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and later the LLC, network and transport layer which are part of the IP layer shown on figure 4, ref. Num "82", "83" are implemented by software drivers which are also called protocol drivers. Binding is the process of associating two pieces of information with each other. With respect to **Holland** the Packet filter service which is shown on figure 2, ref. Num "37" is binding to both the MAC driver which is inherently included in the NIC and the Packet filter is also binding to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num "33" and shown also on figure 3, ref. Num "52". This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num "82" and "83", namely the network layer and the transport layer are all implemented by the protocol driver.)

The network filter service provider [figure 2, ref. Num "37"] implemented as an intermediate driver of the network stack (The network filter service provider is implemented as an intermediate driver because it is bound to the protocol driver [figure 2, ref. Num "33"] and **the media access control driver**.[figure 2, ref. Num "31"] (With respect to **Holland** the Packet filter/an instance of the intrusion detection service which is shown on figure 2, ref. Num "37" is implemented as **an intermediate driver** and bound to the MAC driver which is inherently included in the NIC and to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num "33" and shown also on figure 3, ref. Num "52. This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num "82" and "83", namely the network layer and the transport layer are all implemented by the protocol driver.)**[For the definitions that the examiner used, see the reference U)**

8. **As per claim 9, Holland** discloses the method of performing intrusion prevention as applied to claim 8 above. Furthermore Holland discloses the method further comprising filtering, by the network filter service provider, all data received by the media access control driver prior to passing of the data to the protocol driver. [Figure 2, ref. Num "37" and ref. Num "33"; column 4, lines 41-43] (All data received by the media access control driver which is inherently included in the NIC shown on figure 2, ref. Num "31" is filtered by the packet filter shown on figure 1, ref. Num "37" before it reaches the IP Stack which is inherently includes the protocol driver, since the IP layers namely the network layer shown

on figure 4, ref. Num "82" and the transport layer shown on figure 4, ref. Num "83" are all implemented by the protocol driver. This filtering is done when the incoming data frame is eventually delivered to the host application)

9. **As per claim 10, Holland** discloses the method of performing intrusion prevention as applied to claim 8 above. Furthermore Holland discloses the method further comprising filtering, by the network filter service provider, all data received by the protocol driver prior to passing of the data to the media access control driver.[Figure 2, ref. Num "37" and ref. Num "31"; column 4, lines 43-48](Out going data packets originating from the host application shown on figure 4, ref. Num "40" are processed through the IP stack are filtered as shown on figure 2, ref. Num "37" and eventually transmitted through the MAC which is inherently included in the NIC shown on figure 2, ref. Num "31")

10. **As per claim 12, Holland** discloses the method of performing intrusion prevention as applied to claim 8 above. Furthermore Holland discloses the method wherein binding the network filter service provider to the media access control driver and to the protocol driver occurs upon initialization of the operating system. [Figure 1, ref. Num "32", ref. Num "31" ref. Num "33" and ref. Num "37"]

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a

whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Holland III et al** (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061) in view of **Douglas B.Moran**, (hereinafter referred to as **Moran**) (U.S. Patent No. 6,826,697)

13. **As per claim 1, 4 and 7**, **Holland** discloses **a node** [figure 1, ref. Num "11"' ref. Num "12"] of a **network running an intrusion detection system**,[Column 1, lines 15-18; figure 1, ref. Num "20", ref. Num "19", ref. Num 18"] (The present invention relates in general to network intrusion detection data collection and, in particular, to a system and method for intrusion detection data collection using a network protocol stack multiplexor). **The node comprising**:

- **A central processing unit**; [Column 4, lines 20-23]
- **A memory module for storing data in machine readable format for retrieval and execution by the central processing unit**; [Column 4, lines 23-29]
- **A database for storing a plurality of machine-readable network-exploit signatures; [Column 4, lines 5-8; figure 1, ref. Num "20" or "Hybrid IDS"]** (As shown on figure 1, The network IDS 18, host IDSs 19, and hybrid IDS 20 all collect and analyze a traffic stream to detect any attempts or actual compromises of network or system security. The network IDS 18 focuses on all traffic entering the intranetwork 18 and analyzes that traffic using signature-based and statistical-based

intrusion detection techniques meets the limitation of the "a database for storing a plurality of machine-readable network-exploit signatures".)

- **An operating system** [Figure 2, ref. Num "Kernel"] (The Kernel is the core of an operating system such as Windows 98, Windows NT, Mac OS or Unix. Provides basic services for the other parts of the operating system, making it possible for it to run several programs at once multitasking, read and write files and connect to networks and peripherals.) **comprising**

A network stack comprising a protocol driver,[Figure 1, ref. Num "33"; figure 3, ref. Num "52"; figure 4, ref. Num "82" and ref. Num "83"; Column 6, lines 27-31] (The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and later the LLC, network and transport layer which are part of the IP layer shown on figure 4, ref. Num "82", "83" are implemented by software drivers which are also called protocol drivers)

- **A media access control driver** [figure 2, ref. Num "31"; column 4, lines 53-57] (The MAC driver or media access control driver is also inherently included in the NIC. The MAC or the "media access control driver", also called the network card driver, allows the operating system to talk with the NIC. Windows NT and Windows 95/98 come with MAC drivers for most NICs. The MAC driver got its name from the fact that it operates at the lower level of the OSI model. The second layer of the model, the Data Link layer, is divided into two pieces: the LLC and MAC. The LLC sub layer is implemented in the transport driver while the MAC sub layer is implemented in the NIC) and

•**An instance of the intrusion detection system implemented as an intermediate driver [Figure 2, ref. Num "37"] and bound to the protocol driver** [figure 2, ref. Num "33"] and **the media access control driver**.[figure 2, ref. Num "31"] (With respect to **Holland** the Packet filter/an instance of the intrusion detection service which is shown on figure 2, ref. Num "37" is implemented as an intermediate driver and bound to the MAC driver which is inherently included in the NIC and to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num "33" and shown also on figure 3, ref. Num "52. This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num "82" and "83", namely the network layer and the transport layer are all implemented by the protocol driver.)

Holland does not explicitly discloses

- A database for storing a plurality of machine-readable network-exploit signatures;

However, in the same field of endeavor, **Moran** discloses a database for storing a plurality of machine-readable network-exploit signatures; [Column 8, line 5; figure 3, ref. Num "308"]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of having an attack signatures database as per teachings of **Moran** in to the method analyzing the traffic using signature-based and statistical-based intrusion detection techniques as taught by

Holland, in order strengthen the security by providing an improved system and method for detecting computer intrusions. [See Moran column 3, lines 18-20] **[For the definitions that the examiner used, see the reference U)**

14. **As per claim 2**, the combination of Holland and Moran discloses the method of intrusion detection as applied to claim 1 above. Furthermore Holland discloses the method wherein ,a frame received on a network medium connected to the node [figure 2, ref. Num "13"] is processed by the media access control driver,[figure 2, ref. Num "31"] the intrusion detection system [figure 2, ref. Num "37"] receiving the processed frame directly from the media access control driver.[figure 2, ref. Num "31"]

15. **As per claim 3**, the combination of Holland and Moran discloses the method of intrusion detection as applied to claim 2 above. Furthermore Holland discloses the method wherein the intrusion detection system receiving the processed frame is operable to pass the processed frame to the protocol driver.[Figure 2, ref. Num "37" and ref. Num "33"; Column 4, lines 41-43]] (All data is filtered by the packet filter shown on figure 1, ref. Num "37" before it reaches the IP Stack which is inherently includes the protocol driver, since the IP layers namely the network layer shown on figure 4, ref. Num "82" and the transport layer shown on figure 4, ref. Num "83" are all implemented by the protocol driver. This filtering is done when the incoming data frame is eventually delivered to the host application)

16. **As per claim 5**, the combination of Holland and Moran discloses the method of intrusion detection as applied to claim 1 above. Furthermore Holland discloses the method wherein, a datagram generated by the node is received by the intrusion detection system.[figure 2, ref. Num "37"; column 4, lines 57-58]

17. **As per claim 6**, the combination of Holland and Moran discloses the method of intrusion detection as applied to claim 5 above. Furthermore Holland discloses the method wherein, the intrusion detection system is operable to pass the datagram to the media access control driver. [Figure 2, ref. Num "37" and ref. Num "31"; column 4, lines 43-48; column 4, lines 52-58](Out going data packets originating from the host application shown on figure 4, ref. Num "40" are processed through the IP stack and filtered as shown on figure 2, ref. Num "37" and eventually transmitted through the MAC which is inherently included in the NIC shown on figure 2, ref. Num "31")

Conclusion

18. **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
September 12, 2005

G. Barron

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100